

# ON BILINEAR EXPONENTIAL AND CHARACTER SUMS WITH RECIPROCAL OF POLYNOMIALS

IGOR E. SHPARLINSKI

ABSTRACT. We give nontrivial bounds for the bilinear sums

$$\sum_{u=1}^U \sum_{v=1}^V \alpha_u \beta_v \mathbf{e}_p(u/f(v))$$

where  $\mathbf{e}_p(z)$  is a nontrivial additive character of the prime finite field  $\mathbb{F}_p$  of  $p$  elements, with integers  $U, V$ , a polynomial  $f \in \mathbb{F}_p[X]$  and some complex weights  $\{\alpha_u\}, \{\beta_v\}$ . In particular, for  $f(X) = aX + b$  we obtain new bounds of bilinear sums with Kloosterman fractions. We also obtain new bounds for similar sums with multiplicative characters of  $\mathbb{F}_p$ .

## 1. INTRODUCTION

**1.1. Background and motivation.** Let  $\mathbb{F}_p$  denote the finite field of  $p$  elements, where  $p$  is a sufficiently large prime. Assume that we are given two integers  $1 \leq U, V < p$ , a *convex* set

$$\mathfrak{C} \subseteq [1, U] \times [1, V],$$

a polynomial  $f \in \mathbb{F}_p[X]$  and two sequences of complex “weights”

$$\mathcal{A} = \{\alpha_u\} \quad \text{and} \quad \mathcal{B} = \{\beta_v\} \quad \text{with} \quad |\alpha_u|, |\beta_v| \leq 1.$$

We then consider the bilinear exponential and character sums

$$S_f(\mathcal{A}, \mathcal{B}; \mathfrak{C}) = \sum_{(u,v) \in \mathfrak{C}} \alpha_u \beta_v \mathbf{e}_p(v/f(u)),$$

$$T_f(\mathcal{A}, \mathcal{B}; \mathfrak{C}) = \sum_{(u,v) \in \mathfrak{C}} \alpha_u \beta_v \chi(v + f(u)),$$

where  $\mathbf{e}_p(z) = \exp(2\pi iz/p)$  and  $\chi$  is a fixed nonprincipal character of  $\mathbb{F}_p^*$ , we refer to [16] for a background on exponential sums and multiplicative characters. To simplify the notation we always assume that the zeros of  $f$  in the set  $\{1, \dots, U\}$  are excluded from the summation

---

2010 *Mathematics Subject Classification.* 11D79, 11L07.

*Key words and phrases.* exponential sums, Kloosterman sums, cancellation.

This work was supported in part by ARC Grant DP140100118.

in  $S_f(\mathcal{A}, \mathcal{B}; \mathfrak{C})$  (without adding any extra condition on the summation ranges). Note that with the weights  $\tilde{\alpha}_u = \alpha_u \chi(f(u))$  the sums  $T_f(\mathcal{A}, \mathcal{B}; \mathfrak{C})$  can be written in the same shape as  $S_f(\mathcal{A}, \mathcal{B}; \mathfrak{C})$ , that is,

$$T_f(\mathcal{A}, \mathcal{B}; \mathfrak{C}) = \sum_{(u,v) \in \mathfrak{C}} \tilde{\alpha}_u \beta_v \chi(v/f(u) + 1).$$

Using the well known general bound of bilinear sums, for  $\Pi = [1, U] \times [1, V]$ , we have  $|S_f(\mathcal{A}, \mathcal{B}; \Pi)| \leq \sqrt{UVp}$ , see, for example, [3, Equation (1.4)], and a similar bound for  $T_f(\mathcal{A}, \mathcal{B}; \Pi)$ , which we use as the benchmarks of our progress. Using the same techniques as in the proof of Theorems 2.3 and 2.4 below, it is easy to extend these bounds to arbitrary convex domains  $\mathfrak{C}$  with just a logarithmic loss:

$$(1.1) \quad S_f(\mathcal{A}, \mathcal{B}; \mathfrak{C}) = O\left(\sqrt{UVp} \log p\right)$$

and

$$(1.2) \quad T_f(\mathcal{A}, \mathcal{B}; \mathfrak{C}) = O\left(\sqrt{UVp} \log p\right)$$

(in fact Theorem 2.3 with  $k = 1$  essentially gives (1.1) as well).

In the special case of the weights  $\beta_v = 1$ ,  $v \in [1, V]$ , we simply write  $S_f(\mathcal{A}; \mathfrak{C})$  and  $T_f(\mathcal{A}; \mathfrak{C})$  for the corresponding sums.

Furthermore, for linear polynomials  $f(X) = aX + b$  with  $a, b \in \mathbb{F}_p$  we write

$$K_{a,b}(\mathcal{A}, \mathcal{B}; \mathfrak{C}) = \sum_{(u,v) \in \mathfrak{C}} \alpha_u \beta_v \mathbf{e}_p(v/(au + b)),$$

and

$$K_{a,b}(\mathcal{A}; \mathfrak{C}) = \sum_{(u,v) \in \mathfrak{C}} \alpha_u \mathbf{e}_p(v/(au + b)),$$

for the sums  $S_f(\mathcal{A}, \mathcal{B}; \mathfrak{C})$  and  $S_f(\mathcal{A}; \mathfrak{C})$ , respectively. These sums have a natural interpretation as bilinear Kloosterman sums. We also note that similar trilinear sums (with additional averaging over the modulus  $p$ ) have recently been considered by Bettin & Chandee [1]; we also recall the works of Bourgain [2] and Bourgain & Garaev [4] where different types of bilinear Kloosterman sums are studied.

With these notations, one of the results of [22] can be written as the uniform over  $a \in \mathbb{F}_p^*$  and  $b \in \mathbb{F}_p$  bound

$$(1.3) \quad |K_{a,b}(\mathcal{A}; \mathfrak{C})| \leq (\sqrt{Up} + V)p^{o(1)},$$

as  $p \rightarrow \infty$ . Furthermore, for  $b = 0$ , a stronger bound

$$|K_{a,0}(\mathcal{A}; \mathfrak{C})| \leq (U + V)p^{o(1)},$$

has been given in [21], which is essentially optimal when  $U$  and  $V$  are of the same order.

Note that in [21, 22] only the case of  $\alpha_u = 1$  is considered, but the proofs work without any changes for arbitrary weights  $\mathcal{A}$ .

**1.2. Our results.** Here we obtain a series of results, similar to the bound (1.3) for the sums  $S_f(\mathcal{A}; \mathfrak{C})$ ,  $T_f(\mathcal{A}; \mathfrak{C})$  and  $K_f(\mathcal{A}, \mathcal{B}; \mathfrak{C})$ . These bounds are nontrivial starting from rather small values of  $U$  and  $V$ , in particular in the case when the product  $UV$  is much smaller than  $p$ , which is necessary for the bounds (1.1) and (1.2) to be nontrivial.

Our results are closely related to various questions about congruences with reciprocals and multiplicative congruences with polynomials of the types considered in [4] and [6, 7, 9, 10, 11, 18], respectively. We also use one of the results from [8] which we extend to more generic settings; we hope this may find further applications.

**1.3. Notation.** Throughout the paper, any implied constants in the symbols  $O$ ,  $\ll$  and  $\gg$  may depend on the real parameter  $\varepsilon > 0$  and the integer parameters  $d, \nu \geq 1$ . We recall that the notations  $A = O(B)$ ,  $A \ll B$  and  $A \gg B$  are all equivalent to the statement that the inequality  $|A| \leq cB$  holds with some constant  $c > 0$ .

When we say that a polynomial  $f(X) \in \mathbb{F}_p[X]$  is of degree  $d \geq 1$  we always mean the exact degree, that is, the leading term of  $f$  is  $aX^d$  with  $a \in \mathbb{F}_p^*$ .

The elements of the field  $\mathbb{F}_p$  are assumed to be represented by the set  $\{0, \dots, p-1\}$ . In particular, we often treat elements of  $\mathbb{F}$  as integers or residue classes modulo  $p$ .

## 2. MAIN RESULTS

**2.1. Bilinear exponential sums with polynomials.** We start with extending (1.3) to arbitrary polynomials.

**Theorem 2.1.** *Uniformly over polynomials  $f(X) \in \mathbb{F}_p[X]$  of degree  $d \geq 1$ , we have*

$$|S_f(\mathcal{A}; \mathfrak{C})| \leq p^{d/(d+1)+o(1)} U^{d/2} + V p^{o(1)}.$$

Clearly, for the bound of Theorem 2.1 to be nontrivial it is necessary to have  $U \geq p^\varepsilon$  for some fixed  $\varepsilon > 0$ . However this is not sufficient. For example, and for  $d = 1$  and  $d = 2$  we also need  $UV^2 \geq p^{1+\varepsilon}$  and  $V \geq p^{2/3+\varepsilon}$ , respectively. Furthermore, for  $d \geq 3$ , the bound of

Theorem 2.1 is nontrivial only for rather small values of  $U$ . Namely, for  $d \geq 3$  we also need

$$U \leq p^{-2d/(d+1)(d-2)-\varepsilon} V^{2/(d-2)}.$$

This however can be used to derive a bound which is nontrivial for any  $U$  and  $V$  with

$$U \geq p^\varepsilon \quad \text{and} \quad V \geq p^{d/(d+1)+\varepsilon}.$$

**Corollary 2.2.** *Uniformly over polynomials  $f(X) \in \mathbb{F}_p[X]$  of degree  $d \geq 1$ , we have*

$$|S_f(\mathcal{A}; \mathfrak{C})| \leq \begin{cases} Vp^{o(1)} & \text{if } U \leq V^{2/d} p^{-2/(d+1)}, \\ UV^{1-2/d} p^{2/(d+1)+o(1)} & \text{otherwise.} \end{cases}$$

Unfortunately this method of proof of Theorem 2.1 does not seem to apply to the general sums  $S_f(\mathcal{A}, \mathcal{B}; \mathfrak{C})$  even in the most interesting case when  $\mathfrak{C} = [1, U] \times [1, V]$ . However for powers of linear functions, that is for polynomials of the form  $f(X) = (aX + b)^d \in \mathbb{F}_p[X]$ , we are able to estimate these sums, which we denote by  $S_{a,b,d}(\mathcal{A}, \mathcal{B}; \mathfrak{C})$  in this case.

Using some recent results of Bourgain & Garaev [4] we derive the following estimate:

**Theorem 2.3.** *Uniformly over  $(a, b) \in \mathbb{F}_p^* \times \mathbb{F}_p$  and any fixed integer  $k \geq 1$ , we have*

$$|S_{a,b,d}(\mathcal{A}, \mathcal{B}; \mathfrak{C})| \leq V^{1-1/2k} (U + U^{k/(k+1)} p^{1/2k}) p^{o(1)}.$$

It is easy to see that Theorem 2.3, used with a sufficiently large  $k$ , is nontrivial provided that

$$U^2 V \geq p^{1+\varepsilon} \quad \text{and} \quad V \geq p^\varepsilon,$$

for some fixed  $\varepsilon > 0$ .

**2.2. Bilinear Kloosterman sums.** The bound of Theorem 2.3 with  $d = 1$  also applies to the sums  $K_{a,b}(\mathcal{A}, \mathcal{B}; \mathfrak{C})$ . However, in this case we can obtain more precise results. For example, using some result of Cilleruelo & Garaev [9] in the argument on the proof of Theorem 2.3 we obtain:

**Theorem 2.4.** *Uniformly over  $(a, b) \in \mathbb{F}_p^* \times \mathbb{F}_p$ , we have*

$$|K_{a,b}(\mathcal{A}, \mathcal{B}; \mathfrak{C})| \leq V^{3/4} (U^{7/8} p^{1/8} + U^{1/2} p^{1/4}) p^{o(1)}.$$

It is easy to see that Theorem 2.4 is nontrivial provided that

$$UV^2 \geq p^{1+\varepsilon} \quad \text{and} \quad U^2V \geq p^{1+\varepsilon},$$

for some fixed  $\varepsilon > 0$ .

Finally, using a different approach we also obtain:

**Theorem 2.5.** *Uniformly over  $(a, b) \in \mathbb{F}_p^* \times \mathbb{F}_p$  we have*

$$|K_{a,b}(\mathcal{A}, \mathcal{B}; \mathfrak{C})| \leq UV^{1/2}p^{1/3+o(1)} + U^{1/2}Vp^{o(1)}.$$

Since the proof of Theorem 2.5 uses Theorem 2.1 with  $d = 2$ , it is natural that Theorem 2.5 is nontrivial for

$$U \geq p^\varepsilon \quad \text{and} \quad V \geq p^{2/3+\varepsilon},$$

with some fixed  $\varepsilon > 0$ .

**2.3. Bilinear character sums with polynomials.** Clearly, if  $V \geq p^{1/4+\varepsilon}$  for some fixed  $\varepsilon > 0$  then for the sums  $T_f(\mathcal{A}; \mathfrak{C})$  the Burgess bound, (see [16, Theorem 12.6]), applied to the sum over  $v$  implies a nontrivial estimate of the shape  $|T_f(\mathcal{A}; \mathfrak{C})| \leq UVp^{-\delta}$ , with  $\delta > 0$  that depends only on  $\varepsilon$ .

Here we use some ideas and results from the proof of [8, Theorem 1.2] to estimate the sums  $T_f(\mathcal{A}; \mathfrak{C})$  for smaller values of  $V$ .

**Theorem 2.6.** *For any  $\varepsilon > 0$  there exists some  $\delta > 0$  such that uniformly over polynomials  $f(X) \in \mathbb{F}_p[X]$  of degree  $d \geq 3$ , for*

$$U \geq p^{1/d+\varepsilon} \quad \text{and} \quad V \geq p^{1/4-\delta}$$

*we have*

$$|T_f(\mathcal{A}; \mathfrak{C})| \leq UVp^{-\delta}.$$

We remark that in case of polynomials  $f$  of degree  $d = 1$  much stronger results are given by Karatsuba [17]. The case of  $d = 2$  can also be easily included via the use of classical bounds of Gaussian sums instead of Lemma 4.4, see below. In fact for  $U \geq p^{1/2+\varepsilon}$  more standard approaches work as well, see the discussion in Section 6.

### 3. GENERAL RESULTS

**3.1. Small residues of multiples.** For an integer  $a$  we use  $\rho(a)$  to denote the smallest by absolute value residue of  $a$  modulo  $p$ , that is

$$\rho(a) = \min_{k \in \mathbb{Z}} |a - kp|.$$

We need the following simple statement which follows from the Dirichlet pigeon-hole principle, see [11, Lemma 3.2] or [14, Theorem 2].

**Lemma 3.1.** *For any real numbers  $T_0, \dots, T_d$ , with*

$$p > T_0, \dots, T_d \geq 1 \quad \text{and} \quad T_0 \cdots T_d > p^d,$$

*and any integers  $a_0, \dots, a_d$  there exists an integer  $t$  with  $\gcd(t, p) = 1$  and such that*

$$\rho(a_i t) \ll T_i, \quad i = 0, \dots, d.$$

**3.2. Moments of short character sums.** We recall the classical result of Davenport & Erdős [12], which follows from the Weil bound of multiplicative character sums, see [16, Theorem 11.23].

**Lemma 3.2.** *For a fixed integer  $\nu \geq 1$  and a positive integer  $K < p$ , we have*

$$\sum_{\lambda \in \mathbb{F}_p} \left| \sum_{k=1}^K \chi(\lambda + r_k) \right|^{2\nu} \ll K^{2\nu} p^{1/2} + K^\nu p.$$

**3.3. Congruences with uniformly distributed sequences.** We say that a sequence  $\mathcal{R} = \{r_u\}_{u=1}^U$  of  $U$  elements of  $\mathbb{F}_p$  is  $\eta$ -uniformly distributed modulo  $p$  if uniformly over  $b \in \mathbb{F}_p$  and for any positive integer  $Z < p$

$$(3.1) \quad \begin{aligned} \#\{(u, z) \in [1, U] \times [1, Z] : r_u \equiv b + z \pmod{p}\} \\ = \frac{UZ}{p} + O(\#\mathcal{R}p^{-\eta}). \end{aligned}$$

We now establish a more general form of [8, Lemma 2.9], which in turn is based on some ideas and results of Bourgain, Konyagin and Shparlinski [5] and Shao [20].

**Lemma 3.3.** *For any  $\eta > 0$  there exist some  $\kappa > 0$  such that for positive integers  $L < V < p^{1/2-\eta}$  and any  $\eta$ -uniformly distributed modulo  $p$  sequence  $\mathcal{R} = \{r_u\}_{u=1}^U$  of  $U$  elements of  $\mathbb{F}_p$ , for*

$$N = \#\left\{(\ell_1, \ell_2, u_1, u_2, v_1, v_2) \in \mathcal{L}^2 \times [1, U]^2 \times [1, V]^2 : \frac{v_1 + r_{u_1}}{\ell_1} \equiv \frac{v_2 + r_{u_2}}{\ell_2} \pmod{p}\right\},$$

*where  $\mathcal{L}$  is the set of primes of the interval  $[L, 2L]$ , we have*

$$N \ll LU^2 V p^{-\kappa}.$$

*Proof.* We say that a sequence  $t_1, \dots, t_n \subseteq \mathbb{F}_p$  is  $V$ -spaced if no integers  $1 \leq i < j \leq n$  with  $i \neq j$  and an integer  $v$  with  $|v| \leq V$  satisfy the equality  $t_i + v = t_j$ .

Let  $\mathcal{S}_1$  be the set of indices of the largest  $V$ -separated subsequence of  $\mathcal{U}_0 = \{1, \dots, U\}$ .

Since  $\mathcal{R}$  is  $\eta$ -uniformly distributed modulo  $p$ , we conclude that for some constant  $C$ , depending only on the implied constant in (3.1), each interval  $[b, b+Z] \in [1, p-1]$  of length  $Z \geq Cp^{1-\eta} \geq V$  contains an element of  $\mathcal{R}$ . So, covering  $[1, p]$  by non-overlapping intervals of length  $\lceil Cp^{1-\eta} \rceil$  and choosing an element of the sequence  $\mathcal{R}$  in every second interval (except possibly the last one) we see that  $\#\mathcal{S}_1 \gg p^\eta$ .

We now set  $\mathcal{U}_1 = \mathcal{U}_0 \setminus \mathcal{S}_1$  to be set of indices of remaining elements of  $\mathcal{R}_0$  and proceed inductively, defining  $\mathcal{S}_{k+1}$  as the largest set of indices of a  $V$ -separated subsequence of the sequence  $\{r_u\}_{u \in \mathcal{U}_k}$ , where

$$\mathcal{U}_k = \mathcal{U}_{k-1} \setminus \mathcal{S}_k, \quad k = 1, 2, \dots$$

We terminate, when  $\mathcal{S}_{k+1} \leq p^{\eta/2}$  and then use  $K$  to denote this value of  $k$  and also set  $\mathcal{S}_0 = \mathcal{U}_k$ .

Hence there is a partition

$$\mathcal{U}_0 = \bigcup_{k=0}^K \mathcal{S}_k$$

into  $K \leq Up^{-\eta/2}$  disjoint subsets, where  $\{r_u\}_{u \in \mathcal{S}_k}$  is a  $V$ -separated sequence with  $\#\mathcal{S}_k \geq p^{\eta/2}$ ,  $k = 1, \dots, K$ .

We claim that

$$(3.2) \quad \#\mathcal{S}_0 \ll Up^{-\eta/2}.$$

Indeed, let  $N$  be the smallest number of intervals of length  $V$  that covers the set  $\{r_u\}_{u \in \mathcal{S}_0}$ . Clearly  $\{r_u\}_{u \in \mathcal{S}_0}$  contains a  $V$ -separated set of size  $\lceil N/2 \rceil$ . Hence  $N \ll p^{\eta/2}$ . Since  $\{r_u\}_{u \in \mathcal{S}_0}$  is a subsequence of the sequence  $\mathcal{R}$ , we see that each of such intervals in this covering contains at most  $UV/p + O(Up^{-\eta}) \ll Up^{-\eta}$  elements of  $\mathcal{R}$  and therefore of  $\{r_u\}_{u \in \mathcal{S}_0}$ . Therefore  $\#\mathcal{S}_0 \ll NUp^{-\eta}$  and (3.2) follows. The rest of the proof is identical to that of [8, Lemma 2.9].  $\square$

**3.4. Character sums with uniformly distributed sequences.** We now use the argument of the proof [8, Theorem 1.1] to estimate certainly double character sums with  $\eta$ -uniformly distributed sequences modulo  $p$  (as defined in Section 3.3).

We use the same notation a convex set  $\mathfrak{C} \subseteq [1, U] \times [1, V]$  and weights  $\mathcal{A}$  as in Section 1.1.

**Lemma 3.4.** *For any  $\eta > 0$  there exist some  $\delta > 0$  such that for  $V \geq p^{1/4-\delta}$  any  $\eta$ -uniformly distributed modulo  $p$  sequence  $\mathcal{R} = \{r_u\}_{u=1}^U$  of  $U$  elements of  $\mathbb{F}_p$ , we have*

$$\sum_{(u,v) \in \mathfrak{C}} \alpha_u \chi(v + r_u) \ll UVp^{-\delta}.$$

*Proof.* We note that since  $\mathfrak{C}$  is convex, for each  $u = 1, \dots, U$ , there are integers  $V \geq Y_u \geq X_u \geq 0$  such that

$$\sum_{(u,v) \in \mathfrak{C}} \alpha_u \chi(v + r_u) = \sum_{u=1}^U \alpha_u \sum_{v=X_u+1}^{Y_u} \chi(v + r_u).$$

Clearly we can assume that  $V < p^{1/3}$  as otherwise the Burgess bound (see [16, Theorem 12.6]) implies the desired result. Hence, assuming that  $\eta$  is small enough we see that the conditions of Lemma 3.3 are satisfied for the sequence  $\mathcal{R}$ .

For  $\kappa$  that corresponds the above value of  $\eta$  in Lemma 3.3, we set

$$\gamma = \kappa/5.$$

Let  $K = \lceil p^\gamma \rceil$  and  $L = Vp^{-2\gamma}$ . Also, as in Lemma 3.3 we use  $\mathcal{L}$  to denote the set of primes of the interval  $[L, 2L]$ .

Thus for any integer  $w$  we have

$$\begin{aligned} \sum_{(u,v) \in \mathfrak{C}} \alpha_u \chi(v + r_u) &= \sum_{u=1}^U \alpha_u \left( \sum_{v=X_u+1}^{Y_u} \chi(v + r_u + w) + O(|w|) \right) \\ &= \sum_{(u,v) \in \mathfrak{C}} \alpha_u \chi(v + r_u + w) + O(U|w|). \end{aligned}$$

Therefore

$$\begin{aligned} \sum_{(u,v) \in \mathfrak{C}} \alpha_u \chi(v + r_u) &= \frac{1}{K \# \mathcal{L}} \mathfrak{T} + O(KLU) \\ &\ll \frac{1}{KL} \mathfrak{T} \log p + O(VUp^{-\gamma}), \end{aligned} \tag{3.3}$$

where

$$\mathfrak{T} = \sum_{(u,v) \in \mathfrak{C}} \sum_{\ell \in \mathcal{L}} \sum_{k=1}^K \chi(v + r_u + k\ell).$$

Hence

$$\begin{aligned} \mathfrak{T} &\leq \sum_{(u,v) \in \mathfrak{C}} \sum_{\ell \in \mathcal{L}} \left| \sum_{k=1}^K \chi(v + r_u + k\ell) \right| \\ &\leq \sum_{u=1}^U \sum_{v=1}^V \sum_{\ell \in \mathcal{L}} \left| \sum_{k=1}^K \chi(v + r_u + k\ell) \right| \\ &= \sum_{u=1}^U \sum_{v=1}^V \sum_{\ell \in \mathcal{L}} \left| \sum_{k=1}^K \chi\left(\frac{v + r_u}{\ell} + k\right) \right|. \end{aligned}$$

Collecting together the triples  $(u, v, \ell)$  with the same value  $(v + r_u)/\ell$ , we obtain

$$\mathfrak{T} \leq \sum_{\lambda \in \mathbb{F}_p} I(\lambda) \left| \sum_{k=1}^K \chi(\lambda + k) \right|$$

where

$$I(\lambda) = \# \left\{ (\ell, u, v) \in \mathcal{L} \times [1, U] \times [1, V] : \frac{v + r_u}{\ell} \equiv \lambda \pmod{p} \right\}.$$

We now fix some integer  $\nu \geq 1$ . Writing

$$I(\lambda) = I(\lambda)^{(\nu-1)/\nu} (I(\lambda)^2)^{1/2\nu}$$

and using the Hölder inequality, we derive

$$\mathfrak{T}^{2\nu} = \left( \sum_{\lambda \in \mathbb{F}_p} I(\lambda) \right)^{2\nu-2} \sum_{\lambda \in \mathbb{F}_p} I(\lambda)^2 \sum_{\lambda \in \mathbb{F}_p} \left| \sum_{k=1}^K \chi(v + k) \right|^{2\nu}.$$

We obviously have

$$(3.4) \quad \sum_{\lambda \in \mathbb{F}_p} I(\lambda) \ll \#\mathcal{L}UV \ll LUV.$$

Hence, using Lemma 3.3, we obtain

$$(3.5) \quad \sum_{\lambda \in \mathbb{F}_p} I(\lambda)^2 = N \leq LU^2Vp^{-\kappa}$$

for some  $\kappa > 0$  depending only on  $\eta$  and thus only on  $\varepsilon$ .

Furthermore, taking  $\nu = \lceil \gamma^{-1} \rceil$ , we derive from Lemma 3.2 that

$$(3.6) \quad \sum_{\lambda \in \mathbb{F}_p} \left| \sum_{k=1}^K \chi(v + k) \right|^{2\nu} \ll K^{2\nu} p^{1/2} + K^\nu p \ll K^{2\nu} p^{1/2}.$$

Collecting the bounds (3.4), (3.5) and (3.6), we obtain

$$(3.7) \quad \begin{aligned} \mathfrak{T}^{2\nu} &\ll (LUV)^{2\nu-2} LU^2V K^{2\nu} p^{1/2-\kappa} \\ &= (KLUV)^{2\nu} (LV)^{-1} p^{1/2-\kappa}. \end{aligned}$$

So if  $\delta \leq \kappa/4$ , we see that

$$(LV)^{-1} p^{1/2-\kappa} = V^{-2} p^{1/2-3\kappa/5} \leq p^{-\kappa/10}.$$

Hence we infer from (3.7) that  $\mathfrak{T} \ll (KLUV) p^{-\kappa/20\nu}$ . Substituting this inequality in (3.3) and taking any

$$\delta < \min\{\kappa/4, \kappa/20\nu, \gamma\} = \kappa/20\nu,$$

we conclude the proof.  $\square$

## 4. POLYNOMIAL CONGRUENCES

**4.1. Additive congruences with reciprocals.** We define  $J_{d,k}(a, b; T)$  as the number of solutions to the congruence

$$\sum_{j=1}^{2k} \frac{(-1)^j}{(at_j + b)^d} \equiv 0 \pmod{p}, \quad 1 \leq t_1, \dots, t_{2k} \leq T.$$

First we recall the following result Bourgain & Garaev [4, Proposition 1] (or [4, Theorem 1] if  $d = 1$ ).

**Lemma 4.1.** *For any fixed integer  $k \geq 1$ , for  $1 \leq T < p$ , we have*

$$J_{d,k}(a, b; T) \leq T^{2k+o(1)} p^{-1} + T^{2k^2/(k+1)+o(1)}.$$

For  $d = 1$  we also write  $J_k(a, b; T) = J_{1,k}(a, b; T)$ . Then for  $k = 2$  and  $d = 1$ , the result of Cilleruelo & Garaev [9, Theorem 1] (with  $K = L$ ), see also [4, Corollary 10], yields

**Lemma 4.2.** *For  $1 \leq T < p$ , we have*

$$J_2(a, b; T) \leq T^{7/2+o(1)} p^{-1/2} + T^{2+o(1)}.$$

**4.2. Multiplicative congruences with polynomials.** We need some results about the frequency of small values amongst inverses modulo  $p$  of polynomials. Namely, for a polynomial  $f \in \mathbb{F}_p[X]$  and two positive integers  $U$  and  $Z$  we denote by  $N_f(U, Z)$  the number of solutions to the congruence

$$(4.1) \quad f(u)z \equiv 1 \pmod{p}, \quad 1 \leq u \leq U, \quad 1 \leq z \leq Z.$$

Several approaches to estimating the number of solutions of congruences of this types have recently been considered in [6, 7, 9, 10, 11, 18]. For our purpose, the method of the proof of [9, Theorem 1] is the most suitable.

We now give one of our main technical results, which can be of independent interest.

**Lemma 4.3.** *Uniformly over polynomials  $f(X) \in \mathbb{F}_p[X]$  of degree  $d \geq 1$ , for  $1 \leq U, Z < p$ , we have*

$$N_f(U, Z) \leq (U^{d/2} Z p^{-1/(d+1)} + 1) p^{o(1)}.$$

*Proof.* Without loss of generality we can assume that

$$(4.2) \quad U^{d/2} < p^{1/(d+1)}$$

as otherwise that bound is weaker than the trivial bound  $N_f(U, Z) \ll Z$ .

Let us define positive  $T_0, \dots, T_d$  to satisfy

$$(4.3) \quad T_0 = T_1 U = \dots = T_d U^d \quad \text{and} \quad T_0 \dots T_d = p^d.$$

Clearly the conditions (4.3) allows us to find  $T_i$  explicitly, but for us only the common value  $W = T_i U^i$  is important,  $i = 0, \dots, d$ . It is easy to see that  $W^{d+1} = p^d U^{d(d+1)/2}$ , thus

$$W = p^{d/(d+1)} U^{d/2}.$$

One verifies that (4.2) guarantees that

$$1 \leq W U^{-d} = T_d \leq \dots \leq T_0 = W < p.$$

Thus Lemma 3.1 applies with the above values of  $T_0, \dots, T_d$ .

We now write  $f(X) = a_d X^d + \dots + a_1 X + a_0$  and find  $t \in [1, p-1]$  as in Lemma 3.1. We then define  $g(X) = b_d X^d + \dots + b_1 X + b_0$  with coefficients satisfying

$$b_i \equiv a_i t \pmod{p} \quad \text{and} \quad |b_i| < p/2, \quad i = 0, \dots, d.$$

Then (4.1) is equivalent to

$$(4.4) \quad g(u)z \equiv t \pmod{p}, \quad 1 \leq u \leq U, \quad 1 \leq z \leq Z,$$

and noticing that

$$\rho(g(u)z) \leq (d+1)WZ$$

for all  $(u, z) \in [1, U] \times [1, Z]$ , we see that (4.4) implies

$$g(u)z = t + sp$$

for some  $s = O(WZ)$ . In particular  $z \mid t + sp$  and  $t + sp \neq 0$ . We now recall the well-known bound

$$\tau(m) \leq m^{o(1)}$$

on the number of integer positive divisors  $\tau(m)$  of an integer  $m \neq 0$ , see, for example, [15, Theorem 317].

Hence, for each of the  $O(WZ/p + 1) = O(U^{d/2} Z p^{-1/(d+1)} + 1)$  possible values of  $k$ , there are at most  $p^{o(1)}$  possible values for  $z$ , and for each  $z$  at most  $d$  values for  $u$ . The result now follows.  $\square$

For  $d = 1$ , that is, for a linear polynomial  $f(X) = aX + b$ , the bound of Lemma 4.3 becomes  $(U^{1/2} Z p^{-1/2} + 1) p^{o(1)}$  and corresponds to the estimate from [22].

**4.3. Additive congruences with polynomials.** One of our tools is also the following very special case of a much more general bound of Wooley [24], that applies to polynomials with arbitrary real coefficients.

**Lemma 4.4.** *Uniformly over polynomials  $f(X) \in \mathbb{F}_p[X]$  of degree  $d \geq 3$ , for  $1 \leq U < p$ , we have*

$$\left| \sum_{u=1}^U \mathbf{e}_p(f) \right| \ll U (U^{-1} + pU^{-d})^\sigma$$

where

$$\sigma = \frac{1}{2(d-1)(d-2)}.$$

Clearly, Lemma 4.4 is nontrivial for  $U \geq p^{1/d+\varepsilon}$  for any fixed  $\varepsilon > 0$  and sufficiently large  $p$ . In fact, the classical results of Vinogradov [23] are also sufficient for our purposes.

Now combining Lemma 4.4 with the *Erdős-Turán inequality* (see, for example, [13, Theorem 1.21]), that relates the uniformity of distribution to exponential sums, we immediately obtain:

**Lemma 4.5.** *For any  $\varepsilon > 0$  there exist some  $\eta > 0$  such that uniformly over polynomials  $f(X) \in \mathbb{F}_p[X]$  and  $b \in \mathbb{F}_p$  of degree  $d \geq 3$ , for  $p^{1/d+\varepsilon} \leq U < p$   $1 \leq U, Z < p$ , we have*

$$\begin{aligned} \#\{(u, z) \in [1, U] \times [1, Z] : f(u) \equiv b + z \pmod{p}\} \\ = \frac{UZ}{p} + O(Up^{-\eta}), \end{aligned}$$

where  $\Delta$  is as in Lemma 4.4.

Obviously, the parameter  $b$  does not add any generality to Lemma 4.5 (compared to just  $b = 0$ ), however this is the form in which we apply it. In particular, we see that in the terminology of Section 3.3 the sequence of polynomial values  $\{f(u) : u = 1, \dots, U\}$  is  $\eta$ -uniformly distributed modulo  $p$  provided that  $U \geq p^{1/d+\varepsilon}$ .

## 5. PROOFS OF MAIN RESULTS

**5.1. Proof of Theorem 2.1.** Since  $\mathcal{C}$  is convex, as in the proof of Lemma 3.4 we see that for each  $u = 1, \dots, U$  we there are integers  $V \geq Y_u \geq X_u \geq 0$  such that

$$S_f(\mathcal{A}; \mathfrak{C}) = \sum_{u=1}^U \alpha_u \sum_{v=X_u+1}^{Y_u} \mathbf{e}_p(v/f(u)).$$

We follow the scheme of the proof of [21, Lemma 3]. In particular, we define

$$I = \lfloor \log(2p/V) \rfloor \quad \text{and} \quad J = \lfloor \log(2p) \rfloor.$$

Furthermore, we extend the definition of  $\rho(\alpha)$  from Section 4.2 to rational numbers  $\alpha = u/v$  with  $\gcd(v, p) = 1$ , as  $\rho(\alpha) = |w|$  where  $w$  is the unique integer with  $w \equiv u/v \pmod{p}$  and  $|w| < p/2$ .

Using the bound

$$(5.1) \quad \sum_{v=X_u+1}^{Y_u} \mathbf{e}_p(\alpha v) \ll \min \left\{ V, \frac{p}{\rho(\alpha)} \right\},$$

which holds for any rational  $\alpha$  with the denominator that is not a multiple of  $p$  (see [16, Bound (8.6)]), we derive

$$(5.2) \quad S_f(\mathcal{A}; \mathfrak{C}) = \sum_{u=1}^U \min \left\{ V, \frac{p}{\rho(a/f(u))} \right\}.$$

Hence, we obtain a version of [21, Equation (1)]:

$$(5.3) \quad S_f(\mathcal{A}; \mathfrak{C}) \ll VR + p \sum_{j=I+1}^J Q_j e^{-j},$$

where

$$R = \# \{ u : 1 \leq u \leq U, \rho(a/f(u)) < e^I \},$$

$$Q_j = \# \{ u : 1 \leq u \leq U, e^j \leq \rho(a/f(u)) < e^{j+1} \}.$$

We now see that Lemma 4.3 implies the bounds

$$R \leq (p^{-1/(d+1)} U^{d/2} e^I + 1) p^{o(1)} \leq p^{d/(d+1)} U^{d/2} V^{-1} + p^{o(1)}$$

and

$$Q_j \leq p^{-1/(d+1)+o(1)} U^{d/2} e^j + p^{o(1)}.$$

Substituting these bounds in (5.3), we obtain

$$\begin{aligned} |S_f(\mathcal{A}; \mathfrak{C})| &\ll p^{d/(d+1)+o(1)} U^{d/2} + V p^{o(1)} \\ &\quad + p^{1+o(1)} \sum_{j=I+1}^J (p^{-1/(d+1)} U^{d/2} e^j + 1) e^{-j} \\ &= (p^{d/(d+1)} U^{d/2} + V + J p^{d/(d+1)} U^{d/2} + p^1 e^{-I}) p^{o(1)} \\ &= p^{d/(d+1)+o(1)} U^{d/2} + V p^{o(1)}, \end{aligned}$$

which concludes the proof.

**5.2. Proof of Corollary 2.2.** Note that we can assume that  $V > p^{d/(d+1)}$  as otherwise the bound is trivial.

We now choose some parameter  $K \geq 1$  and slice the summation region  $\mathfrak{C}$  vertically into  $K$  domains of the form  $\mathfrak{C} \cap [A+1, A+\tilde{U}]$  with  $\tilde{U} = U/K + O(1)$ . Applying Theorem 2.1 to the polynomial  $f(A+X)$  to estimate the sum over  $\mathfrak{C} \cap [A+1, A+\tilde{U}]$ , we obtain

$$|S_f(\mathcal{A}; \mathfrak{C})| \leq K (p^{d/(d+1)}(U/K)^{d/2} + V) p^{o(1)}.$$

We now set

$$K = \lceil UV^{-2/d} p^{2/(d+1)} \rceil$$

and conclude the proof.

**5.3. Proof of Theorem 2.3.** Since  $\mathfrak{C}$  is convex, for each  $v \in [1, V]$  there are some integers  $U \geq Y_v \geq X_v \geq 0$  such that for an integer  $u$  the condition  $(u, v) \in \mathfrak{C}$  is equivalent to  $X_u < u \leq Y_u$ . Hence, using the orthogonality of exponential functions, we obtain

$$\begin{aligned} \sum_{u: (u,v) \in \mathfrak{C}} \alpha_u \mathbf{e}_p(v/(au+b)^d) &= \sum_{u=X_v+1}^{Y_v} \alpha_u \mathbf{e}_p(v/(au+b)^d) \\ &= \sum_{u=1}^U \alpha_u \mathbf{e}_p(v/(au+b)^d) \sum_{x=X_v+1}^{Y_v} \frac{1}{p} \sum_{\lambda=-(p-1)/2}^{(p-1)/2} \mathbf{e}_p(\lambda(x-u)) \\ &= \frac{1}{p} \sum_{\lambda=-(p-1)/2}^{(p-1)/2} \sum_{u=1}^U \alpha_u \mathbf{e}_p(v/(au+b)^d - \lambda u) \sum_{x=X_v+1}^{Y_v} \mathbf{e}_p(\lambda x). \end{aligned}$$

Recalling (5.1), we obtain

$$\begin{aligned} &\left| \sum_{u: (u,v) \in \mathfrak{C}} \alpha_u \mathbf{e}_p(v/(au+b)^d) \right| \\ &\ll \sum_{\lambda=-(p-1)/2}^{(p-1)/2} \frac{1}{|\lambda|+1} \left| \sum_{u=1}^U \alpha_u \mathbf{e}_p(v/(au+b)^d - \lambda u) \right|. \end{aligned}$$

Thus, we conclude that

$$\begin{aligned} (5.4) \quad |K_{a,b}(\mathcal{A}, \mathcal{B}; \mathfrak{C})| &\leq \sum_{v=1}^V \left| \sum_{u: (u,v) \in \mathfrak{C}} \alpha_u \mathbf{e}_p(v/(au+b)^d) \right| \\ &\ll \sum_{\lambda=-(p-1)/2}^{(p-1)/2} \frac{1}{|\lambda|+1} W(\lambda), \end{aligned}$$

where

$$W(\lambda) = \sum_{v=1}^V \left| \sum_{u=1}^U \alpha_u(\lambda) \mathbf{e}_p(v/(au+b)^d) \right|$$

with  $\alpha_u(\lambda) = \alpha_u \mathbf{e}_p(-\lambda u)$ . Using the Hölder inequality and the extending the range of summation over  $v$  to the whole field  $\mathbb{F}_p$ , we derive

$$\begin{aligned} W(\lambda)^{2k} &\leq V^{2k-1} \sum_{v=1}^V \left| \sum_{u=1}^U \alpha_u(\lambda) \mathbf{e}_p(v/(au+b)^d) \right|^{2k} \\ &\leq V^{2k-1} \sum_{v \in \mathbb{F}_p} \left| \sum_{u=1}^U \alpha_u(\lambda) \mathbf{e}_p(v/(au+b)^d) \right|^{2k}. \end{aligned}$$

Using that for any complex  $\xi$  we have  $|\xi|^2 = \xi \bar{\xi}$ , expanding the  $(2k)$ -th power and changing the order of summation, we derive

$$\begin{aligned} W(\lambda)^{2k} &\leq V^{2k-1} \sum_{u_1, \dots, u_{2k}=1}^U \prod_{i=1}^k \alpha_{u_{2i-1}}(\lambda) \overline{\alpha_{u_{2i}}(\lambda)} \\ &\quad \sum_{v \in \mathbb{F}_p} \mathbf{e}_p \left( v \sum_{j=1}^{2k} \frac{(-1)^j}{(au_j+b)^d} \right) \\ &\leq V^{2k-1} \sum_{u_1, \dots, u_{2k}=1}^U \sum_{v \in \mathbb{F}_p} \mathbf{e}_p \left( v \sum_{j=1}^{2k} \frac{(-1)^j}{(au_j+b)^d} \right) \\ &= V^{2k-1} p J_{d,k}(a, b; U), \end{aligned}$$

where  $J_{d,k}(a, b; U)$  is as in Section 4.1. From Lemma 4.1 we now easily derive

$$(5.5) \quad W(\lambda) \leq V^{1-1/2k} (U + U^{k/(k+1)} p^{1/2k}) p^{o(1)},$$

which we substitute in (5.4) and conclude the proof.

**5.4. Proof of Theorem 2.4.** We proceed exactly as in the proof of Theorem 2.3 with  $k = 2$  but use Lemma 4.2 instead of Lemma 4.1, getting

$$W(\lambda)^4 \leq V^3 p (U^{7/2+o(1)} p^{-1/2} + U^{2+o(1)})$$

instead of (5.5).

5.5. **Proof of Theorem 2.5.** Writing

$$|K_{a,b}(\mathcal{A}, \mathcal{B}; \mathfrak{C})| \leq \sum_{v=1}^V \left| \sum_{u: (u,v) \in \mathfrak{C}} \alpha_u \mathbf{e}_p(v/(au+b)) \right|$$

and using the Cauchy inequality, we obtain

$$\begin{aligned} |K_{a,b}(\mathcal{A}, \mathcal{B}; \mathfrak{C})|^2 &\leq V \sum_{v=1}^V \left| \sum_{u: (u,v) \in \mathfrak{C}} \alpha_u \mathbf{e}_p(v/(au+b)) \right|^2 \\ &= V \sum_{v=1}^V \sum_{u: (u,v) \in \mathfrak{C}} \sum_{w: (w,v) \in \mathfrak{C}} \alpha_u \alpha_w \mathbf{e}_p \left( \frac{v}{au+b} - \frac{v}{aw+b} \right) \\ &= V \sum_{v=1}^V \sum_{u: (u,v) \in \mathfrak{C}} \sum_{w: (w,v) \in \mathfrak{C}} \alpha_u \alpha_w \mathbf{e}_p \left( \frac{av(w-u)}{(au+b)(aw+b)} \right). \end{aligned}$$

Hence, changing the order of summation again, we obtain

$$|K_{a,b}(\mathcal{A}, \mathcal{B}; \mathfrak{C})|^2 \leq V \sum_{u,w=1}^U \left| \sum_{v \in \mathcal{I}(u,w)} \mathbf{e}_p \left( \frac{av(w-u)}{(au+b)(aw+b)} \right) \right|,$$

where  $\mathcal{I}(u, w)$  is the set of integers  $v \in [1, V]$  with  $(u, v) \in \mathfrak{C}$  and  $(w, v) \in \mathfrak{C}$ . Therefore, writing  $w = u + z$ , we derive

$$\begin{aligned} &|K_{a,b}(\mathcal{A}, \mathcal{B}; \mathfrak{C})|^2 \\ (5.6) \quad &\leq V \sum_{z=-U}^U \sum_{u=1}^U \left| \sum_{v \in \mathcal{I}(u, u+z)} \mathbf{e}_p \left( \frac{avz}{(au+b)(a(u+z)+b)} \right) \right|. \end{aligned}$$

Now, for  $z = 0$  we estimate the double sum over  $u$  and  $v$  trivially as  $UV$ . Otherwise, we note that  $\mathcal{I}(u, u+z)$  is an interval and then proceed exactly as in the proof of Theorem 2.1 arriving to (5.2). Hence, for every  $z \neq 0$ , to the sum over  $u$  and  $v$  in (5.6) we obtain the bound of Theorem 2.1 with  $d = 2$ . Collecting these estimates, we obtain

$$\begin{aligned} |K_{a,b}(\mathcal{A}, \mathcal{B}; \mathfrak{C})|^2 &\leq UV^2 + UV (p^{2/3+o(1)}U + Vp^{o(1)}) \\ &= U^2Vp^{2/3+o(1)} + UV^2p^{o(1)}, \end{aligned}$$

and the result now follows.

5.6. **Proof of Theorem 2.6.** The result follows immediately from the combinations of Lemmas 3.4 and 4.5.

## 6. COMMENTS

Theorems 2.1 and 2.6 also improve the generic bounds (1.1), (6.1) and (1.2) for a very wide range of parameters.

Our arguments also apply to the sums

$$\sum_{(u,v) \in \mathfrak{C}} \alpha_u \beta_v \mathbf{e}_p(vf(u)), \quad f \in \mathbb{F}_p[X],$$

where one can use the results from [7, 10] instead of Lemma 4.3. However, after an application of the Cauchy inequality and “smoothing” the summation over  $u$  one can also use the bounds of Wooley [24] directly, while our approach does not seem to give any substantial gain.

We also remark that (5.2) immediately implies the bound

$$(6.1) \quad S_f(\mathcal{A}; \mathfrak{C}) \ll p \log p,$$

which is better than (1.1) (however (1.1) applies to more general sums).

It is easy to see that for  $d = 1$  each of Theorems 2.3, 2.4 and 2.5 has a range of parameters where it is stronger than the other two (and the bound (6.1)).

It easy to see that for  $d = 1$  each of the Theorems 2.3, 2.4 and 2.5 has a range of parameters where it is stronger than the other two (and the generic bound (6.1)).

In Table 6.1 we give examples which illustrate this (‘\*’ indicates the winning bound and ‘—’ indicates that the corresponding bound is trivial. Note that in all out examples  $UV \leq p$ , the bound (6.1) is always trivial and so is not included in Table 6.1. We also suppress the terms  $p^{o(1)}$ ). In the case of Theorem 2.3, we also give the optimal values of  $k$ .

$(U, V)$	Thm. 2.3	Thm. 2.4	Thm. 2.5
$(p^{2/5}, p^{3/10})$	* $p^{419/600}$ ( $k = 14$ or $15$ )	—	—
$(p^{2/5}, p^{2/5})$	$p^{111/140}$ ( $k = 6$ or $7$ )	* $p^{31/40}$	—
$(p^{1/5}, p^{4/5})$	$p^{59/60}$ ( $k = 2$ or $3$ )	$p^{19/20}$	* $p^{14/15}$

TABLE 6.1. Comparison between Theorems 2.3, 2.4 and 2.5

It is certainly interesting to obtain nontrivial estimates on the sums  $S_f(\mathcal{A}, \mathcal{B}; \mathfrak{C})$  and  $T_f(\mathcal{A}, \mathcal{B}; \mathfrak{C})$  in full generality or even on more general sums, where  $f(X)$  is a rational function rather than a polynomial. For example, for the sums  $S_f(\mathcal{A}, \mathcal{B}; \mathfrak{C})$ , to get such result one needs appropriate extensions of the bounds on  $N_f(U, Z)$  in Section 4.2 to

arbitrary rational functions. Obtaining such bounds is certainly of independent interest. In fact it is easy to see that a standard application of the Weil bound of exponential sums with rational functions, see, for example, [19], leads to the asymptotic formula

$$(6.2) \quad N_f(U, Z) = \frac{UZ}{p} + O(p^{1/2}(\log p)^2),$$

for any nontrivial rational function  $f$ . It is obvious that (6.2) is nontrivial for  $U \geq p^{1/2+\varepsilon}$ , with any fixed  $\varepsilon$  and thus can be used to estimate the sum  $S_f(\mathcal{A}; \mathfrak{C})$  and  $S_f(\mathcal{A}, \mathcal{B}; \mathfrak{C})$ . Furthermore, in this range one can simply use the Cauchy inequality to obtain a full analogue of (5.4) for the sums  $S_f(\mathcal{A}, \mathcal{B}; \mathfrak{C})$ , and then apply to the inner sums the Weil bound for incomplete sums with rational functions. The same standard approach also works for the sums  $T_f(\mathcal{A}, \mathcal{B}; \mathfrak{C})$ . However we are mostly interested in small values of  $U$ , beyond the reach of the Weil bound.

## REFERENCES

- [1] S. Bettin and V. Chandee, ‘Trilinear forms with Kloosterman fractions’, *Preprint*, 2015 (available from <http://arxiv.org/abs/1502.00769>).
- [2] J. Bourgain, ‘More on the sum-product phenomenon in prime fields and its applications’, *Int. J. Number Theory*, **1** (2005), 1–32.
- [3] J. Bourgain and M. Z. Garaev, ‘On a variant of sum-product estimates and explicit exponential sum bounds in prime fields’, *Math. Proc. Cambr. Phil. Soc.*, **146** (2008), 1–21.
- [4] J. Bourgain and M. Z. Garaev, ‘Sumsets of reciprocals in prime fields and multilinear Kloosterman sums’, *Izvestiya: Mathematics*, **78** (2014), 656–707.
- [5] J. Bourgain, S. V. Konyagin and I. E. Shparlinski, ‘Character sums and deterministic polynomial root finding in finite fields’, *Math. Comp.*, (to appear).
- [6] M.-C. Chang, ‘Sparsity of the intersection of polynomial images of an interval’, *Acta Arith.*, **165** (2014), 243–249.
- [7] M.-C. Chang, J. Cilleruelo, M. Z. Garaev, J. Hernández, I. E. Shparlinski and A. Zumalacárregui, ‘Points on curves in small boxes and applications’, *Michigan Math. J.*, **63** (2014), 503–534.
- [8] M.-C. Chang and I. E. Shparlinski, ‘Double character sums over subgroups and intervals’, *Bull. Aust. Math. Soc.*, **90** (2014), 376–390.
- [9] J. Cilleruelo and M. Z. Garaev, ‘Concentration of points on two and three dimensional modular hyperbolas and applications’, *Geom. and Funct. Anal.*, **21** (2011), 892–904.
- [10] J. Cilleruelo, M. Z. Garaev, A. Ostafe and I. E. Shparlinski, ‘On the concentration of points of polynomial maps and applications’, *Math. Zeit.*, **272** (2012), 825–837.
- [11] J. Cilleruelo, I. E. Shparlinski and A. Zumalacárregui, ‘Isomorphism classes of elliptic curves over a finite field in some thin families’, *Math. Res. Letters*, **19** (2012), 335–343.

- [12] H. Davenport and P. Erdős, ‘The distribution of quadratic and higher residues’, *Publ. Math. Debrecen*, **2** (1952), 252–265.
- [13] M. Drmota and R. Tichy, *Sequences, discrepancies and applications*, Springer-Verlag, Berlin, 1997.
- [14] D. Gómez-Pérez and J. Gutierrez, ‘On the linear complexity and lattice test of nonlinear pseudorandom number generators’, *Applied Algebra and Number Theory*, Cambridge Univ. Press, Cambridge, 2014, 91–101.
- [15] G. H. Hardy and E. M. Wright, *An introduction to the theory of numbers*, Oxford Univ. Press, Oxford, 1979.
- [16] H. Iwaniec and E. Kowalski, *Analytic number theory*, American Mathematical Society, Providence, RI, 2004.
- [17] A. A. Karatsuba, ‘The distribution of values of Dirichlet characters on additive sequences’, *Doklady Acad. Sci. USSR*, **319** (1991), 543–545 (in Russian).
- [18] B. Kerr, ‘Solutions to polynomial congruences in well shaped sets’, *Bull. Aust. Math. Soc.*, **88** (2013), 435–447.
- [19] C. J. Moreno and O. Moreno, ‘Exponential sums and Goppa codes, 1’, *Proc. Amer. Math. Soc.*, **111** (1991), 523–531.
- [20] X. Shao, ‘Character sums over unions of intervals’, *Forum Math.*, (to appear).
- [21] I. E. Shparlinski, ‘Exponential sums with Farey fractions’, *Bull. Polish Acad. Sci. Math.*, **57** (2009), 101–107.
- [22] I. E. Shparlinski, ‘Linear congruences with ratios’, *Preprint*, 2015 (available from <http://arxiv.org/abs/1503.03196>).
- [23] I. M. Vinogradov, *The method of trigonometrical sums in the theory of numberst*, Trav. Inst. Math. Stekloff, vol. 23, 1947.
- [24] T. D. Wooley, ‘Translation invariance, exponential sums, and Warings problem’, *Proc. Intern. Congress of Mathematicians*, Seoul, 2014, 505–529.

DEPARTMENT OF PURE MATHEMATICS, UNIVERSITY OF NEW SOUTH WALES,  
SYDNEY, NSW 2052, AUSTRALIA

*E-mail address:* igor.shparlinski@unsw.edu.au